**УДК 004.05**

# ЗАЩИТА ИНТЕРНЕТ-СИСТЕМЫ ОТ ВЗЛОМА ПОСТОРОННИМИ ЛИЦАМИ

***Н.А. МЕДВЕДЕВ***
***(Представлено: канд. техн. наук, доц. И.Б. БУРАЧЕНОК)***

*В данной статье рассматривается методы взлома интернет-системы для получения информации и подробное описание представляющих наибольшую угрозу. Рассмотрены методы защиты интернет-сервиса от подобных несанкционированных атак.*

**Введение.** Сегодня одной из самых серьёзных проблем в сфере информационно-вычислительных систем является защита информации в интернете. Современные люди не только разговаривают и переписываются посредством интернета, но и осуществляют различные финансовые операции, заказывают товары, услуги, пользуются кредитными карточками, проводят платежи, т. е. совершают множество действий, требующих обеспечения конфиденциальности и защиты. Попав в руки злоумышленника конфиденциальные данные способны привести к опасным последствиям. Поэтому к безопасности интернет-систем предъявляются высокие требования и рассмотрение методов по обеспечению защиты такой системы является актуальным.

Целью представленной статьи является выбор и обоснование наиболее эффективных методов защиты интернет-сервисов от несанкционированных атак.

Вначале, проанализируем основные методы взлома интернет-систем и выявим предоставляющие наибольшую угрозу.

Взлом пароля – специальная процедура методичного угадывания зашифрованного слова или фразы, которую злоумышленник пытается получить из централизованной базы данных [1]. Данные действия обычно применяются в 2 случаях, когда необходимо:

– восстановить забытый пароль;

– узнать пароль другого пользователя системы без его ведома для незаконных действий с его учетными данными.

Что касается сферы Quality assurance (QA), то процесс взлома пароля обычно используется с целью, осуществления проверки безопасности приложения, отыскав максимальное количество существующих уязвимостей в его системе [1].

В сегодняшних реалиях развития IT-сообщества, многие программисты поставили себе за цель создать особые алгоритмы, которые могли бы взламывать установленные пароли за минимальные временные промежутки. Больше половины инструментов, представленных в данном сегменте программирования, ориентируются на вход в систему на основе максимального количества допустимых словесных и буквенных комбинаций. Если перед хакером очень сложный пароль (структура которого состоит из особой комбинации цифр, букв и специальных символов), то его взлом может занять от нескольких часов до нескольких недель. Имеются и особые программы со встроенными словарями паролей, однако успешность применения подобных инструментов несколько ниже, так как с одновременным подбором комбинаций ключевые запросы сохраняются в приложении, а это занимает определенное время [1].

Существует 15 способов взлома пароля интернет-системы [2].

1. Перебор по словарю –полный перебор всех предполагаемых паролей.
2. Брутфорс –полный перебор всех символов в указанном диапазоне.
3. Фишинг – получение данных через поддельный сайт, где пользователь вводит персональные данные для входа.
4. Вирусы – использование специализированной программы по получению данных отправкой на другой компьютер.
5. Плечевой серфинг – получение данных методом просмотра другого пользователя.
6. Сканер портов – просмотр незащищённых портов и их использование для проникновения в систему жертвы.
7. Радужная таблица – метод использования для вскрытия паролей, преобразованных при помощи сложно обратимой хеш-функции, а также для атак на симметричные шифры на основе известного открытого текста.
8. Оффлайновый взлом – взлом путём восстановления пароля из кэша браузера. Требуется физическое использование системой жертвы.
9. Социальная инженерия – получение данных путём убеждения выдачи самим пользователем.
10. Гибридная атака – взлом методом комбинации брутфорса и словаря.
11. Взлом секретных вопросов – взлом путём угадывания ответа по секретным вопросам.

12. Цепь Маркова – последовательность случайных событий с конечным или счётным числом исходов, где вероятность наступления каждого события зависит от состояния, достигнутого в предыдущем событии.
13. Гибридный словарь – взлом методом словаря, а затем комбинации с брутфорсом.
14. Спайдеринг – поиск всех информации жертвы с последующим использованием брутфорса.
15. Keyloggers – занесение вируса-трояна для отлова всех символов, нажатых пользователем.

Если рассмотрим подробнее следующие виды вышеприведённых атак:

Брутфорс – взлом пароля путём перебора всех возможных вариантов ключа. Особенностью данного метода является возможность применения данного способа против любого практически используемого шифра. Однако такая возможность существует лишь теоретически, порой требуя нереалистичные временные и ресурсные затраты. Если пространство решений очень большое, то такой вид атаки может не дать результатов в течение нескольких лет или даже веков [3].

Радужная таблица – специальный вариант таблиц поиска для обращения криптографических хеш-функций, использующий механизм разумного компромисса между временем поиска по таблице и занимаемой памятью. Радужные таблицы используются для вскрытия паролей, преобразованных при помощи сложнообратимой хеш-функции, а также для атак на симметричные шифры на основе известного открытого текста. Использование функции формирования ключа с применением «соли» (об этом рассмотрим далее) делает эту атаку неосуществимой [4].

Цепь Маркова – последовательность случайных событий с конечным или счётным числом исходов, где вероятность наступления каждого события зависит от состояния, достигнутого в предыдущем событии. Характеризуется тем свойством, что при фиксированном настоящем – будущее независимо от прошлого [5]. В Марковских цепочках атак хакеры собирают определенную базу паролей. Вначале они разбивают пароли на 2-3 длинных слога символов, а затем разрабатывают новый алфавит. Таким образом, метод в основном основан на сопоставлении различных наборов паролей, пока он не найдёт исходный пароль. Это очень похоже на словарную атаку, но более продвинутую.

Вышеперечисленные атаки показывают, что возникает необходимость в применении мер по защите интернет-систем, выполнив определенную последовательность действий. В первую очередь, необходимо произвести в базе данных полное разделение пользователей на группы с разграничением уровня доступа. Затем использовать для пользователей следующие методы для осложнения взлома системы и пароля:

Хеширование – функция, осуществляющая преобразование массива входных данных произвольной длины в (выходную) битовую строку установленной длины, выполняемое определённым алгоритмом. Преобразование, производимое хеш-функцией, называется хешированием. Исходные данные называются входным массивом, «ключом» или «сообщением». Результат преобразования (выходные данные) называется «хешем», «хеш-кодом», «хеш-суммой», «сводкой сообщения» [6]. Этот способ позволяет в случае взлома не раскрыть базу паролей и значительно повышает надёжность системы. Однако в связи с использованием метода радужной таблицы рекомендуется использовать хеширование с «солью».

«Соль» – это случайную составляющая, добавляемая в конец или в начало пароля перед операцией хеширования [7]. При этом, как показано в примере выше, всякий раз получаются совершенно разные строки из одного и того же хеш-кода пароля. Соль не обязательно держать в секрете. Просто при использовании случайной величины для построения хеш-кода таблицы поиска, обратные таблицы поиска и радужные таблицы становятся неэффективными. Злоумышленник не узнает заранее, какая будет «соль», поэтому он не может предварительно вычислить таблицу поиска или радужную таблицу. Если пароль каждого пользователя хешируется с помощью разной «соли», атака с использованием обратной таблицы поиска также не будет работать [7].

Многофакторная аутентификация (МФА, англ. multi-factor authentication, MFA) – расширенная аутентификация, метод контроля доступа к компьютеру, в котором пользователю для получения доступа к информации необходимо предъявить более одного «доказательства механизма аутентификации». К категориям таких доказательств относят:

– знание – информация, которую знает субъект, например, пароль, ПИН-код.
– владение – вещь, которой обладает субъект.
– свойство, которым обладает субъект, например, биометрия, природные уникальные отличия: лицо, отпечатки пальцев, радужная оболочка глаз, капиллярные узоры, последовательность ДНК [8].

Среди видов аутентификации отдельно рассмотрим двухфакторную аутентификацию.

Двухфакторная аутентификация (ДФА) – тип многофакторной аутентификации [9]. ДФА представляет собой технологию, обеспечивающую идентификацию пользователей с помощью комбинации двух различных компонентов. Примеры ДФА: авторизация, используемая крупнейшей в мире поисковой системой интернета Google и авторизация – на уровне приложений Microsoft. Когда пользователь осуществляет вход с нового устройства, помимо аутентификации по имени-паролю его просят ввести шестизначный (Google) или восьмизначный (Microsoft) код подтверждения. Абонент может получить его по SMS оповещению, с помощью голосового звонка на его телефон, причем, код подтверждения может быть взят из

заранее составленного реестра разовых кодов или новый одноразовый пароль может быть сгенерирован приложением-аутентификатором за короткий промежуток времени. Метод выбирается в настройках аккаунта Google или Microsoft соответственно [9].

ReCAPTCHA – система, разработанная в университете Карнеги – Меллона для защиты веб-сайтов от интернет-ботов и одновременной помощи в оцифровке текстов книг. Принцип работы ReCAPTCHA кроется в недопущении податься обману программой распознавания текста. Второе слово берется из источника, требующего распознавания, например, книги. Проверка и прохождение «капчи» осуществляется по тому слову, которое известно системе. Неизвестное второе слово вводить не обязательно. Второе слово, введённое пользователем, сохраняется в системе и используется в качестве возможного варианта распознавания. Окончательное распознавание слова производится путём выбора слова, наиболее часто используемого для ввода. Система reCAPTCHA предоставляет пользователям изображения для распознавания и собирает результаты, после чего передаёт их организаторам оцифровки материалов [9].

**Заключение.** В результате проведённого исследования были проанализированы основные виды взлома интернет-системы и методы её защиты от подобных действий. На основании проведённого анализа планируется внедрение защиты для проекта, основной задачей которого является предоставление условий распространения неигрового ПО с возможностью запустить купленные приложения с помощью специального лаунчера.

ЛИТЕРАТУРА

1. 10 самых популярных программ для взлома паролей в 2019 году. [Электронный ресурс] / TestMatick. – Режим доступа: https://testmatick.com/ru/10-samyh-populyarnyh-programm-dlya-vzloma-parolej-v-2019-godu/. – Дата доступа: 15.09.2020.
2. Password Cracking Techniques Used By Hackers in 2020. [Электронный ресурс] / TechViral. – Режим доступа: https://techviral.net/top-password-cracking-techniques-used-by-hackers/ – Дата доступа: 18.09.2019.
3. Полный перебор [Электронный ресурс] / Wikipedia. – Режим доступа: https://ru.wikipedia.org/wiki/Полный_перебор – Дата доступа: 16.09.2020.
4. Радужная таблица [Электронный ресурс] / Wikipedia. – Режим доступа: https://ru.wikipedia.org/wiki/Радужная_таблица – Дата доступа: 16.09.2020.
5. Цепь Маркова [Электронный ресурс] / Wikipedia. – Режим доступа: https://ru.wikipedia.org/wiki//Цепь_Маркова – Дата доступа: 16.09.2020.
6. Хеш-функция. [Электронный ресурс] / Wikipedia. – Режим доступа: https://ru.wikipedia.org/wiki/Хеш-функция: 17.09.2020.
7. «Соленое» хеширование паролей: делаем правильно [Электронный ресурс] / Интернет-технологии. – Режим доступа: https://www.internet-technologies.ru/articles/solenoe-heshirovanie-paroley-delaem-pravilno.html – Дата доступа: 17.09.2020.
8. Многофакторная аутентификация [Электронный ресурс] / Wikipedia. – Режим доступа: https://ru.wikipedia.org/wiki/Многофакторная_аутентификация – Дата доступа: 17.09.2020.
9. ReCAPTCHA [Электронный ресурс] / Wikipedia. – Режим доступа: https://ru.wikipedia.org/wiki/ReCAPTCHA – Дата доступа: 17.09.2020.